Exhibit A

Exhibit A

FIRST INTERIM REPORT OF JOHN J. RAY III TO THE INDEPENDENT DIRECTORS ON CONTROL FAILURES AT THE FTX EXCHANGES

April 9, 2023

TABLE OF CONTENTS

I. Introduction

FTX Trading Ltd. ("FTX.com" and, together with its U.S. counterpart, FTX.US, the "FTX exchanges") was among the world's largest cryptocurrency exchanges, where millions of customers bought, sold and traded crypto assets. The FTX exchanges gained international prominence for their popularity among users, their high-profile acquisitions and celebrity endorsements, and the public image of Sam Bankman-Fried, their co-founder and CEO, as a philanthropist who worked to enhance standards, disclosure, oversight, and customer protection in the crypto industry.[1] On November 11, 2022, however, capping a stunning collapse that began just nine days earlier with the revelation of financial weakness at their affiliated trading firm, Alameda Research LLC ("Alameda"), the FTX exchanges and certain entities under common ownership (the "FTX Group")[2] filed for bankruptcy (the "Chapter 11 Cases"). Within weeks, Bankman-Fried was charged with perpetrating a multibillion-dollar fraud through the FTX Group with at least three senior insiders, who have pleaded guilty in connection with the scheme.

When the Chapter 11 Cases were first filed, the Debtors[3] identified five core objectives: (1) implementation of controls, (2) asset protection and recovery, (3) transparency and investigation, (4) efficiency and coordination with any non-U.S. proceedings and

---

[1] *See* David Yaffe-Bellany, *A Crypto Emperor's Vision: No Pants, His Rules*, N.Y. TIMES, May 14, 2022, https://www.nytimes.com/2022/05/14/business/sam-bankman-fried-ftx-crypto.html?.

[2] The "FTX Group" refers to FTX Trading Ltd., West Realm Shires Services Inc., d/b/a FTX.US, Alameda Research LLC, and their directly and indirectly owned subsidiaries.

[3] The Debtors comprise the approximately one hundred entities associated with the FTX Group listed at https://restructuring.ra.kroll.com/FTX.

(5) maximization of value.[4] It is in furtherance of these core objectives, particularly transparency, that this first interim report is issued. The Debtors plan to issue supplemental reports which describe the cause and effect of the pre-petition events which lead up to the Chapter 11 Cases.

In working to achieve their objectives, the Debtors have had to overcome unusual obstacles due to the FTX Group's lack of appropriate record keeping and controls in critical areas, including, among others, management and governance, finance and accounting, as well as digital asset management, information security and cybersecurity. Normally, in a bankruptcy involving a business of the size and complexity of the FTX Group, particularly a business that handles customer and investor funds, there are readily identifiable records, data sources, and processes that can be used to identify and safeguard assets of the estate. Not so with the FTX Group.

Upon assuming control, the Debtors found a pervasive lack of records and other evidence at the FTX Group of where or how fiat currency and digital assets could be found or accessed, and extensive commingling of assets. This required the Debtors to start from scratch, in many cases, simply to identify the assets and liabilities of the estate, much less to protect and recover the assets to maximize the estate's value. This challenge was magnified by the fact that the Debtors took over amidst a massive cyberattack, itself a product of the FTX Group's lack of controls, that drained approximately $432 million worth of assets on the date of the bankruptcy

[4] First Day Declaration of John Ray III, Dkt 24 ("First Day Declaration") ¶ 6. *See also* Presentation to the Official Committee of Unsecured Creditors, Dkt 507 at 7; Presentation to the Official Committee of Unsecured Creditors, Dkt 792 (describing efforts to assess exchange shortfalls); Presentation to the Official Committee of Unsecured Creditors, Dkt 1101 (describing statement of financial affairs).

petition (the "November 2022 Breach"),[5] and threatened far larger losses absent measures the Debtors immediately implemented to secure the computing environment.

Despite the public image it sought to create of a responsible business, the FTX Group was tightly controlled by a small group of individuals who showed little interest in instituting an appropriate oversight or control framework. These individuals stifled dissent, commingled and misused corporate and customer funds, lied to third parties about their business, joked internally about their tendency to lose track of millions of dollars in assets, and thereby caused the FTX Group to collapse as swiftly as it had grown. In this regard, while the FTX Group's failure is novel in the unprecedented scale of harm it caused in a nascent industry, many of its root causes are familiar: hubris, incompetence, and greed.

This first interim report provides a high-level overview of certain of the FTX Group's control failures in the areas of (i) management and governance, (ii) finance and accounting, and (iii) digital asset management, information security and cybersecurity. The report does not address all control failures in these or other areas. The Debtors continue to learn new information daily as their work progresses and expect to report additional findings in due course.

II. Background

The following is a brief description of the FTX Group entities most relevant to this interim report.

A. Alameda

Founded in 2017 by Bankman-Fried and Gary Wang, Alameda operated as a "crypto hedge fund" that traded and speculated in crypto assets and related loans and securities

[5] All crypto asset values set forth in this report are as of the petition date, November 11, 2022.

for the account of its owners, Bankman-Fried (90%) and Wang (10%).[6] Alameda also offered over-the-counter trading services and made and managed other debt and equity investments. Beginning in October 2021, Caroline Ellison acted variously as CEO and co-CEO of Alameda, which was organized in the State of Delaware.

B. FTX.com

Founded in 2019 by Bankman-Fried and Wang, FTX.com was a digital asset trading platform and exchange that was organized in Antigua and represented as being off-limits to U.S. users.[7] FTX.com was operated, at the most senior level, by Bankman-Fried, Wang, and Nishad Singh, who had worked at Alameda and joined FTX.com soon after it was launched. By November 2022, FTX.com had more than seven million registered users around the world.

C. FTX.US

Founded in January 2020 by Bankman-Fried, Wang, and Singh, FTX.US was an exchange for spot trading in digital assets and tokens in the United States. The FTX.US platform was organized in the State of Delaware. By November 2022, FTX.US had over one million U.S. users.[8]

III. Scope of Review

A. Retention of Advisers

In connection with the Chapter 11 Cases and related matters, the Debtors have retained a number of advisers, including:[9]

---

6 First Day Declaration ¶ 22.

7 *See id.* ¶ 33.

8 *Id.* ¶ 21.

9 This summary is limited to the advisers, and the work these advisers are performing, on the control failures that are relevant to this interim report. As noted in the Debtors' Chapter 11 filings, some of these advisers have additional responsibilities, and the Debtors have retained additional advisers beyond those listed here to assist with other important matters of the estate.

- **Legal:** The Debtors retained Sullivan & Cromwell LLP as lead counsel to assist in the filing and prosecution of the Chapter 11 Cases, investigating potential causes of action and avenues of recovery for the Debtors' estate, and responding to requests from government authorities, among other matters. The Debtors also retained Quinn Emanuel Urquhart & Sullivan LLP as Special Counsel to assist the Debtors and the Board in litigating bankruptcy-related matters against third parties, and investigating and prosecuting certain claims, including asset recovery actions.

- **Restructuring, asset identification and forensic accounting:** The Debtors retained Alvarez & Marsal North America, LLC ("A&M") as their restructuring adviser to assist in identifying, quantifying, and securing liquid and crypto assets, investments, and other property of the Debtors' estate, as well as development of ongoing business plans and supporting the overall restructuring process. The Debtors also retained AlixPartners LLP ("AlixPartners") to assist in tracing and analyzing financial and accounting data, including trading activity and FTX Group internal transfers, and re-constructing historical financial statements for each Debtor entity.

- **Cybersecurity, computer engineering, and cryptography:** The Debtors retained Sygnia, Inc. ("Sygnia") to secure their computing environment following the November 2022 Breach; to identify and secure the Debtors' remaining digital assets; to investigate the November 2022 Breach; and to perform technical and forensic analysis in support of the Debtors' other ongoing work to recover assets.

- **Blockchain analytics:** The Debtors retained TRM Labs, Inc. ("TRM") and Chainalysis Inc. ("Chainalysis") to engage in blockchain analysis to assist A&M and Sygnia in identifying crypto assets of the Debtors, and to monitor crypto assets stolen in the November 2022 Breach, including in order to work with law enforcement and other third parties to attempt to freeze and recover the stolen assets.

Identifying and recovering assets of the Debtors' estate, and identifying potential claims of the estate, requires extensive coordination among these advisers, particularly given the FTX Group's lack of adequate record keeping and extensive commingling of assets.

B. Data Collection

To date, the Debtors have reviewed over one million documents collected from Debtor entities around the world, including communications (*e.g.*, Slack, Signal, email) and other documents (*e.g.*, Excel spreadsheets, Google Drive documents). The Debtors have also been engaged in substantial analysis of FTX Group customer transaction data, which is housed in databases that are over one petabyte (*i.e.*, 1000 terabytes) in size. The Debtors' review of relevant documents and customer transaction data remains ongoing.

The Debtors have also reviewed and analyzed the FTX Group's available financial records. These include QuickBooks, which certain entities in the FTX Group used as their general ledgers; certain bank statements; financial statements; tax returns; promissory notes evidencing intercompany loans; spreadsheets recording real estate transactions, political and charitable contributions, and venture investments; and Slack channels devoted to expense reimbursements and related matters.

Finally, the Debtors have analyzed a small set of laptops and other electronic devices of certain employees of the FTX Group, and continue to collect such devices. The set of electronic devices in the Debtors' possession does not include those known to have belonged to Bankman-Fried and other key insiders that are currently in the possession of the Bahamian Joint Provisional Liquidators ("JPLs") and are the subject of ongoing discussion between the Debtors and the JPLs.

C. Witnesses

To date, the Debtors have conducted interviews of 19 employees of the FTX Group, and received substantial information through counsel for five others. These include interviews of employees who worked in Policy and Regulatory Strategy, Information Technology, Controllers, Administration, Legal, Compliance, and Data Science and Engineering, among others. The Debtors continue to identify, interview, and collect information from potentially relevant witnesses.

While Singh, Wang, and Ellison have pleaded guilty pursuant to cooperation agreements with the Justice Department, it is generally not feasible for the Debtors to interview them on key subjects until after the ongoing criminal prosecution of Bankman-Fried has concluded. Wang has provided discrete assistance to the Debtors' financial and technical advisors.

IV. Review of Control Failures

The FTX Group's control failures created an environment in which a handful of employees had, among them, virtually limitless power to direct transfers of fiat currency and crypto assets and to hire and fire employees, with no effective oversight or controls to act as checks on how they exercised those powers. These employees, particularly Bankman-Fried, deprioritized or rejected advice to improve the FTX Group's control framework, exposing the exchanges to grave harm from both external bad actors and their own misconduct.

A. Lack of Management and Governance Controls

The FTX Group lacked appropriate management, governance, and organizational structure. As a result, a primary objective of the Debtors has been to institute an appropriate governance framework from the outset of the bankruptcy.

1. FTX Group Management and Governance

The management and governance of the FTX Group was largely limited to Bankman-Fried, Singh, and Wang. Among them, Bankman-Fried was viewed as having the final voice in all significant decisions, and Singh and Wang largely deferred to him.[10] These three individuals, not long out of college and with no experience in risk management or running a business, controlled nearly every significant aspect of the FTX Group. With isolated exceptions, including for FTX.US Derivatives ("LedgerX"), a non-Debtor entity it acquired in late 2021, FTX Japan, a Debtor acquired in 2022, and Embed Clearing LLC, a non-Debtor acquired in 2022, the FTX Group lacked independent or experienced finance, accounting, human resources, information security, or cybersecurity personnel or leadership, and lacked any internal audit function whatsoever. Board oversight, moreover, was also effectively non-existent.

[10] *See, e.g.*, *SEC* v. *Caroline Ellison et al.*, 22-cv-10794 (S.D.N.Y. Dec. 21, 2022), Compl. ¶¶ 21, 25, 45(b), 45(c), 46, 67, 96, Dkt 1; *SEC* v. *Nishad Singh*, 23-cv-01691 (S.D.N.Y. Feb. 28, 2023), Compl. ¶¶ 8, 9, 32, 34, 40, 50-51, 67, 90, 100, Dkt 1.

Most major decision-making and authority sat with Bankman-Fried, Singh, and Wang, and numerous significant responsibilities were not delegated to other executives or managers even where such individuals had been hired. Commenting on Wang's and Singh's control over the FTX Group's technology development and architecture, an FTX Group executive stated that "if Nishad [Singh] got hit by a bus, the whole company would be done. Same issue with Gary [Wang]."

Efforts to clarify corporate responsibilities and enhance compliance were not welcome and resulted in backlash. For example, the President of FTX.US resigned following a protracted disagreement with Bankman-Fried and Singh over the lack of appropriate delegation of authority, formal management structure, and key hires at FTX.US; after raising these issues directly with them, his bonus was drastically reduced and senior internal counsel instructed him to apologize to Bankman-Fried for raising the concerns, which he refused to do. Similarly, less than three months after being hired, and shortly after learning about Alameda's use of a North Dimension bank account to send money to customers of the FTX exchanges, a lawyer within the FTX Group was summarily terminated after expressing concerns about Alameda's lack of corporate controls, capable leadership, and risk management.

Echoing its lack of appropriate management and governance structure, the FTX Group lacked an appropriate organizational structure. Rather than having an ultimate parent company able to serve as a central point for decision-making that could also direct and control its subsidiaries, the FTX Group was organized as a web of parallel corporate chains with various owners and interests, all under the ultimate control of Bankman-Fried.

The FTX Group's lack of management and governance controls also manifested in the absence of any comprehensive organizational chart of the FTX Group entities prior to the end of 2021, and the lack of any tracking of intercompany relationships and ownership of

particular entities. At the time of the bankruptcy filing, the FTX Group did not even have current and complete lists of who its employees were.

2. Debtors' Management and Governance

A primary objective of the Debtors was to institute an appropriate management, governance, and structural framework at the outset of the bankruptcy. To do so, the Debtors arranged the conduct of the Chapter 11 Cases into four groups of businesses, or "Silos," for organizational purposes: (a) Debtor West Realm Shires Inc. and its Debtor and non-Debtor subsidiaries (the "WRS Silo"), which includes the businesses known as FTX.US, LedgerX, FTX.US Derivatives, FTX.US Capital Markets, and Embed Clearing, among other businesses; (b) Debtor Alameda Research LLC and its Debtor subsidiaries (the "Alameda Silo"); (c) Debtor Clifton Bay Investments LLC, Debtor Clifton Bay Investments Ltd., Debtor Island Bay Ventures Inc. and Debtor FTX Ventures Ltd. (the "Ventures Silo"); and (d) Debtor FTX Trading Ltd. and its Debtor and non-Debtor subsidiaries (the "Dotcom Silo"), including the exchanges doing business as "FTX.com" and similar exchanges in non-U.S. jurisdictions. The Debtors then moved expeditiously to build a Board of Directors that, for the first time, would provide independent oversight of the disparate corporate chains that constituted the FTX Group.

As previously set forth in filings in the Chapter 11 Cases, the Debtors appointed a board of directors (the "Board") consisting of five directors with respective silo responsibilities.[11] These directors were wholly independent from the FTX Group, and have a wealth of experience in complicated restructuring matters well suited to the Debtors' present

[11] First Day Declaration ¶¶ 46-47.

circumstances.[12] The Board meets effectively on a weekly or more frequent basis on matters of common interest of the Silo directors, including the objectives set forth above.[13]

The Debtors appointed John J. Ray III as their Chief Executive Officer, Mary Cilia as their Chief Financial Officer, Kathryn Schultea as their Chief Administrative Officer, and Raj Perubhatla as their Chief Information Officer. These officers each have extensive experience in providing crisis management services, including work relating to complex financial and operational restructurings, to distressed and under-performing companies. Collectively, these executives have over 125 years of experience, including at senior management levels of public companies.

B. Lack of Financial and Accounting Controls

At its peak, the FTX Group operated in 250 jurisdictions, controlled tens of billions of dollars of assets across its various companies, engaged in as many as 26 million transactions per day, and had millions of users. Despite these asset levels and transaction volumes, the FTX Group lacked fundamental financial and accounting controls. Reconstruction of the Debtors' balance sheets is an ongoing, bottom-up exercise that continues to require significant effort by professionals.

---

[12] *Id.* The Director of the WRS Silo is Mitchell I. Sonkin, a Senior Advisor to MBIA Insurance Corporation. The Director of the Alameda Silo is Matthew R. Rosenberg, a Partner at Lincoln Park Advisors. The Director of the Ventures Silo is Rishi Jain, a Managing Director and Co-Head of the Western Region of Accordion. The Director of the Dotcom Silo, and the Lead Independent Director, is the Honorable Joseph J. Farnan, who served for almost three decades as a United States District Judge for the District of Delaware.

[13] At this phase in the Chapter 11 Cases, the Debtors are focused on asset recovery and maximization of value for all stakeholders through the eventual reorganization or sale of the Debtors' complex array of businesses, investments and property around the world. The Debtors believe that all Silos benefit from this central administration process and full visibility of the assets being obtained, and the various sales processes being run, with all Silo Directors participating in the relevant decision-making processes in order to flag any inter-Silo issues early. At a later stage in the Chapter 11 Cases, when the Debtors' assets have been appropriately marshaled and secured, the Board and Debtors will turn their focus to distributional matters. The Board has also implemented appropriate procedures for the resolution of any conflicts of interest among the Silos and if necessary as the case progresses, any Silo may engage independent counsel in connection with the resolution of intercompany claims which, as the Debtors have previously noted, are likely to be complex but are still in the process of being assessed.

1. Lack of Key Personnel, Departments and Policies

The FTX Group did not have personnel who were experienced and knowledgeable enough to account accurately for assets and liabilities, understand and hedge against risk, or compile and validate financial reports. Key executive functions, including those of Chief Financial Officer, Chief Risk Officer, Global Controller and Chief Internal Auditor, were missing at some or all critical entities. Nor did the FTX Group have any dedicated financial risk, audit, or treasury departments. Although certain of the FTX Group entities nominally employed individuals responsible for accounting at those entities, in many instances, those individuals lacked the requisite expertise and had little or no internal staff. As a general matter, policies and procedures relating to accounting, financial reporting, treasury management, and risk management did not exist, were incomplete, or were highly generic and not appropriate for a firm handling substantial financial assets.

Indeed, in late December 2020, when the FTX Group learned, in connection with exploring a potential direct listing on NASDAQ, that FTX.US would have to be audited, and that this audit would include a review of policies and procedures, senior FTX Group personnel scrambled to cobble together purported policies that could be shown to auditors. In requesting the assistance of certain employees in quickly writing policies, FTX Group management informed them that because the "auditors [would] spend time in understanding and reviewing [FTX] internal processes," internal controls would have to be documented. FTX Group management asked employees "well-versed with" "parts of the [work]flow" to provide first drafts of policies and procedures in a mere 24 hours. It is unclear to what extent the resulting policies—which were prepared by editing off-the-shelf precedents provided by the FTX Group's outside accountants—reflected the reality of the FTX Group's business, but they were never formally promulgated, and no employees were ever trained on them.

The FTX Group principally relied on a small outside accounting firm to perform almost all of its basic accounting functions. Although the outside accountants' public profile is limited, it appears to have a small number of employees and no specialized knowledge relating to cryptocurrencies or international financial markets. There is no evidence that the FTX Group ever performed an evaluation of whether its outside accountants were appropriate for their role given the scale and complexity of the FTX Group's business, or whether they possessed sufficient expertise to account for the wide array of products in which the FTX Group transacted.

2. Lack of Appropriate Accounting Systems

Companies with operations as large and complex as those of the FTX Group normally employ either an advanced off-the-shelf Enterprise Resource Planning ("ERP")[14] system (*e.g.*, Oracle Fusion Cloud ERP, SAP S/4HANA Cloud) or a sophisticated proprietary system tailored to the accounting needs of the business such as, for a crypto exchange or trading business, a system tailored to the crypto assets in which the business transacted. Any appropriate accounting system should be capable of handling large volumes of data to accurately record, process, and report financial statement information (balance sheet/income statement) as well as operational information (actual versus budgeted spending), and to store key supporting materials. To minimize the risk of data integrity errors and the need for manual processing of transactions, data should flow automatically into the accounting system from core systems of the business, with transactions recorded based on appropriate accounting criteria and logic. None of the FTX Group companies employed such an accounting system.

Fifty-six entities within the FTX Group did not produce financial statements of any kind. Thirty-five FTX Group entities used QuickBooks as their accounting system and

[14] An ERP system is a type of software system that helps an organization automate and manage core business processes for optimal performance. ERP software coordinates the flow of data among a company's business processes, streamlining operations across the enterprise.

relied on a hodgepodge of Google documents, Slack communications, shared drives, and Excel spreadsheets and other non-enterprise solutions to manage their assets and liabilities. QuickBooks is an accounting software package designed for small and mid-sized businesses, new businesses, and freelancers.[15] QuickBooks was not designed to address the needs of a large and complex business like that of the FTX Group, which handled billions of dollars of securities, fiat currency, and cryptocurrency transactions across multiple continents and platforms.

As a result of the FTX Group's poor controls, and the inherent limitations of QuickBooks software for use in a large and complex business, the FTX Group did not employ QuickBooks in a manner that would allow it to maintain accurate financial records. For example, QuickBooks did not interface directly with the FTX Group's core systems. Data had to be transported from the FTX Group systems into QuickBooks manually, generally by outside accountants who did not have access to the source data to validate that they had completely and accurately transferred the data into QuickBooks. Furthermore, because they processed large volumes of data only manually, a great deal of transaction detail (*e.g.*, the purpose of a transaction) was either populated *en masse*, or omitted entirely. Substantial accounts and positions went untracked in QuickBooks. Digital asset transactions were tracked in QuickBooks using the generic entry "investments in cryptocurrency," but detailed recordkeeping reflecting what those cryptocurrency investments actually consisted of did not exist in QuickBooks, making reconciliation with other data sources extremely challenging or impossible. Approximately 80,000 transactions were simply left as unprocessed accounting entries in catch-all QuickBooks accounts titled "Ask My Accountant." Further complicating matters,

[15] *See* INTUIT QUICKBOOKS, https://quickbooks.intuit.com/ (last visited Apr. 4, 2023).

QuickBooks entries were often made months after transactions occurred, rendering impossible real-time financial reporting and risk management.

Alameda often had difficulty understanding what its positions were, let alone hedging or accounting for them. For the vast majority of assets, Alameda's recordkeeping was so poor that it is difficult to determine how positions were marked. A June 2022 "Portfolio summary" purporting to model cryptocurrency positions held by Alameda stated, with respect to valuation inputs for certain tokens, that Alameda personnel should "come up with some numbers? idk." In an internal communication, Bankman-Fried described Alameda as "hilariously beyond any threshold of any auditor being able to even get partially through an audit," adding:

> Alameda is unauditable. I don't mean this in the sense of "a major accounting firm will have reservations about auditing it"; I mean this in the sense of "*we* are only able to ballpark what its balances are, let alone something like a comprehensive transaction history." We sometimes find $50m of assets lying around that we lost track of; such is life.

Bankman-Fried's statements evidence the challenges a competent audit firm would have had to overcome to audit Alameda's business.

3. Inadequate Reporting and Documentation

A large number of FTX Group entities did not close financial reporting periods on a timely basis, and back-end checks to identify and correct material errors (*e.g.*, secondary review of transactions over a certain size, reconciliations of bank accounts, cryptocurrency wallets transactions, and other off-exchange positions) did not occur. These and other deficiencies resulted in numerous, often substantial, positions either not being recorded or being recorded in vague or inaccurate ways.

Key accounting reports necessary to understand the FTX Group's assets and liabilities, such as statements of cash flows, statements of equity, intercompany and related party

transaction matrices, and schedules of customer entitlements, did not exist or were not prepared regularly. Important treasury reports, such as reports on daily liquidity, daily settlement, funding mismatches, concentration risk, and liability profiles, did not exist or were not prepared regularly. Copies of key documentation—including executed loan agreements, intercompany agreements, acquisition and investment documents, bank and brokerage account statements, and contract and account information of all types—were incomplete, inaccurate, contradictory, or missing entirely. Thousands of deposit checks were collected from the FTX Group's offices, some stale-dated for months, due to the failure of personnel to deposit checks in the ordinary course; instead, deposit checks collected like junk mail. As discussed in greater detail below, the FTX Group did not maintain reliable lists of bank or trading accounts, cryptocurrency wallets, or authorized signatories. The Debtors have had to construct this historical data from scratch and make sense of the numerous resulting discrepancies, anomalies, and undocumented positions.

Although the FTX Group consisted of many, separate entities, transfers of funds among those entities were not properly documented, rendering tracing of funds extremely challenging. To make matters worse, Slack, Signal, and other informal methods of communication were frequently used to document approvals. Signal and Telegram were at times utilized in communications with both internal and external parties with "disappearing messages" enabled, rendering any historical review impossible. Expenses and invoices of the FTX Group were submitted on Slack and were approved by "emoji." These informal, ephemeral messaging systems were used to procure approvals for transfers in the tens of millions of dollars, leaving only informal records of such transfers, or no records at all.

Numerous loans were executed between former insiders and Alameda without contemporaneous documentation, and funds were disbursed pursuant to those purported loans with no clear record of their purpose. In one instance, an insider entered into an agreement to

purchase a piece of real estate. The funds used to purchase that property, however, were wired directly from Alameda and FTX Digital Markets Ltd. ("FTX DM"), a Bahamas-based entity which was owned by, and had obtained the funds from, FTX Trading Ltd. Only four months after the real estate purchase had closed did the employee enter into a promissory note with Alameda in which he undertook to repay the funds used to purchase the property. Other insiders received purported loans from Alameda for which no promissory notes exist.

4. Trading Records from Other Exchanges

While the FTX Group maintained over a thousand accounts on external digital asset trading platforms in jurisdictions around the world, many of which held significant assets at various points in time, it had no comprehensive, centralized source of information reflecting the purpose of these accounts, or the credentials to access them. Many of these accounts were opened using names and email addresses that were not obviously linked to any of the FTX Group entities. Other accounts were opened using pseudonymous email addresses, in the names of shell companies created for these purposes, or in the names of individuals (including individuals with no direct connection to the FTX Group).

The Debtors have been working to identify and access these external accounts in order to secure the Debtors' assets and extract historical trading data. Obtaining such access has required significant document review, interviews with current and former employees, and engagement with the external platforms. In many instances, accounts belonging to the Debtors have been seized, locked, or frozen, requiring further coordination with the platforms and foreign government agencies to provide adequate proof of ownership and authorization to access the accounts.

5. Intercompany Transactions

The FTX Group did not observe any discernable corporate formalities when it came to intercompany transactions. Assets and liabilities were routinely shuffled among the FTX Group entities and insiders without proper process or documentation. Alameda routinely provided funding for corporate expenditures (*e.g.*, paying salaries and other business expenses) whether for Alameda, for various other Debtors, or for FTX DM, and for venture investments or acquisitions whether for Alameda or for various other Debtors. Alameda also transferred funds to insiders to fund personal investments, political contributions, and other expenditures—some of which were nominally "papered" as personal loans with below-market interest rates and a balloon payment due years in the future.

Intercompany and insider transfers were often recorded on the QuickBooks general ledgers in a manner that was inconsistent with the apparent purpose of the transfers. For example, an Alameda bank account transferred tens of millions of dollars to a personal bank account of Bankman-Fried in 2021 and 2022. Although the transfers were documented in promissory notes as loans from Alameda to Bankman-Fried, they were recorded on the general ledger as "Investment in Subsidiaries: Investments-Cryptocurrency." The Debtors have identified examples of intercompany transactions that do not balance to each other (*i.e.*, where the amounts "due to" and "due from" do not balance across the relevant entities). North Dimension, a shell company owned by Alameda, frequently recorded cash transfers to Alameda accounts in the general ledger with the description "interco transfer reflecting bank wire," without otherwise stating the purpose or substance of the transaction.

In addition to these inconsistencies, many intercompany transactions recorded in the QuickBooks general ledgers involved digital assets, but critical records regarding which digital assets were transferred, and at what values they were transferred, were not maintained in

QuickBooks. Multiple intercompany transactions were recorded in QuickBooks by grouping many transactions together in summary batch entries without sufficient information to identify or properly account for the underlying transactions. Compounding the issue, these batch entries were then recorded under generalized account names in QuickBooks such as "investments in cryptocurrency," as described above. The cumulative impact is that these intercompany transactions as recorded in QuickBooks are difficult to reconcile with underlying documentation, and have required substantial additional investigation to understand and properly account for.

6. Extraordinary Privileges Granted to Alameda

Alameda was a customer of FTX.com, trading for its own account as well as engaging in market-making activities, and, in that capacity, it was granted extraordinary privileges by the FTX Group.[16] As detailed below, the FTX Group configured the codebase of FTX.com and associated customer databases to grant Alameda an effectively limitless ability to trade and withdraw assets from the exchange regardless of the size of Alameda's account balance, and to exempt Alameda from the auto-liquidation process that applied to other customers. Any number of different controls routinely implemented by financial institutions and exchanges in established financial markets would be expected to have prevented, detected, and escalated these secret privileges to personnel in control functions with sufficient independence and authority to address the issue.[17]

[16] FTX Group granted the same privileges to Alameda on FTX.US. Because the Debtors' investigation is ongoing as to whether or to what extent Alameda made use of these privileges on FTX.US, this discussion focuses on FTX.com.

[17] For instance, at a financial institution, these privileges would be expected to be identified by the finance department, as part of balance activity reports and margin balance monitoring; the market risk department, via VAR calculations and funding risk metrics; and the accounting department, through reconciliations of account-level balances against independently calculated aggregate exchange balances; and by having compliance, information technology, risk management, and finance departments that are segregated and independent from traders and other front-line business personnel.

The FTX Group not only failed to disclose these privileges to its customers or the public, but affirmatively misrepresented Alameda's privileged status relative to that of other customers. On July 31, 2019—the same day Singh altered the codebase to allow Alameda to withdraw apparently unlimited amounts of crypto assets from FTX.com, and a week after he altered it to effectively exempt Alameda from auto-liquidation—Bankman-Fried claimed on Twitter that Alameda's account was "just like everyone else's and "Alameda's incentive is just for FTX to do as well as possible."[18] As recently as September 2022, in interviews with reporters, Bankman-Fried claimed that Alameda was a "wholly separate entity" and Ellison claimed that Alameda was "arm's-length and [did not] get any different treatment from other market makers."[19]

a. FTX customers and auto-liquidation processes

In general, there were two types of customers on FTX.com: retail customers and market makers (*i.e.*, liquidity providers that stand ready to buy or sell to satisfy market demand). As to both types of customers, the exchange implemented automatic liquidation processes such that if the customer's account balance fell below a certain threshold, then the customer's existing positions on the exchange would be liquidated (*i.e.*, sold off) until the account balance became net-positive again.

For retail customers, the auto-liquidation process was triggered if the customer's account balance approached zero. Market-makers and certain other preferred customers were

---

[18] Sam Bankman-Fried, Twitter (July 31, 2019), *at* https://twitter.com/bitshine_/status/1156665108174651392?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1156696100729806849%7Ctwgr%5E4bccfdc775938ec4496be7f2a64f95301cbc3e7b%7Ctwcon%5Es2_&ref_url=https%3A%2F%2Fwww.forbes.com%2Fadvisor%2Finvesting%2Fcryptocurrency%2Fwhat-happened-to-ftx%2F (responding to a Twitter user's question about how Bankman-Fried would "resolve the conflict of interest of running [his] own derivative exchange, AND actively trading against the market at the same time").

[19] Annie Massa, Anna Irrera, and Hannah Miller, *Quant Shop with Ties to FTX Powers Bankman-Fried's Crypto Empire*, BLOOMBERG NEWS (Sept. 14, 2022).

provided lines of credit in amounts that varied by customer up to a maximum of $150 million; for those customers, the auto-liquidation process would be triggered if the account became negative and approached the pre-set borrowing limit.

Apart from auto-liquidation processes that prevented customers from trading on the exchange if their balance went below a given threshold, through the operation of its code, FTX.com did not allow customers—except, as set forth below, Alameda—to withdraw assets from the exchange in excess of the amount of their net-positive account balance.

b. Alameda's privileges

Contrary to the public claims of FTX Group management, the FTX Group exempted Alameda from the automatic processes set forth above in multiple ways. Specifically, one of the privileges secretly granted to Alameda, executed through a setting known as "*borrow*," permitted Alameda alone to trade on FTX.com effectively without regard to the size of its overall negative position. *Borrow* was a field in the customer account settings within the FTX.com exchange's customer databases that contained a value for each customer representing how much the customer could "borrow"—*i.e.*, whether and to what extent the customer's account balance could become net-negative without triggering trade restrictions or the FTX.com exchange's auto-liquidation processes. As of the petition date, on FTX.com:

- Most retail customers had a *borrow* value of zero;
- Certain preferred customers and market makers had a *borrow* value greater than zero and in amounts up to $150 million;

- Alameda alone had a *borrow* value set to $65 billion.[20]

The second and third privileges secretly granted to Alameda, known as "*can_withdraw_below_borrow*," and "*allow_negative*," provided Alameda the unique ability to withdraw an unlimited amount of crypto assets from FTX.com even when its account balance was net-negative. Singh added these features to the codebase of the FTX.com exchange on July 23, 2019 and July 31, 2019, respectively. It appears that Alameda's *can_withdraw_below_borrow* privilege was quickly supplanted by the addition to the codebase of *allow_negative*, which operated in essentially the same manner and controlled in the event of conflict with the settings for *can_withdraw_below_borrow*.[21]

Allow_negative referred to a field in the FTX.com exchange's customer databases that, if set to "true" for a particular customer, (i) allowed the customer to *withdraw* an unlimited amount of crypto assets from the FTX.com exchange while having a net-negative account balance (as opposed to merely "borrow") and (ii) exempted the customer from the FTX.com exchange's automatic liquidation processes. As of the petition date, Alameda was the only customer on FTX.com for which *allow_negative* was set to "true." When taken together, Alameda's $65 billion *borrow* and *allow_negative* settings gave it the unique ability to trade and

[20] Due to the FTX Group's failure to maintain appropriate database logs, it is not possible to determine precisely when these particular *borrow* values for Alameda were configured, or by whom. In interviews, one FTX Group employee recalled that, in approximately the summer of 2022, he discovered a configuration that gave Alameda a line of credit in a very large amount, and raised the issue with Singh, who responded that he would reduce the amount to $1 billion (an amount that would still be approximately seven times larger than that of any customer or market maker on the exchange). Due to the lack of database logs, it is unclear what Alameda's *borrow* value was set to at the time, or to what extent Singh made any change to reduce it. Nonetheless, database records reflect that as of the petition date, Alameda's *borrow* limit was set to $65 billion.

[21] While it appears that *can_withdraw_below_borrow* was thus rendered obsolete by Singh's addition of *allow_negative*, the Debtors currently understand that the *borrow* privilege granted to Alameda continued to remain relevant because Alameda would still need a net-positive account balance (after accounting for the specified *borrow* value) in order to actually trade on the exchange.

withdraw virtually unlimited assets, regardless of the size of its account balance and without risk of its positions being liquidated.

The Debtors' investigation of extraordinary privileges granted to Alameda remains ongoing.

C. Lack of Digital Asset Management, Information Security & Cybersecurity Controls

The Debtors identified extensive deficiencies in the FTX Group's controls with respect to digital asset management, information security, and cybersecurity. These deficiencies were particularly surprising given that the FTX Group's business and reputation depended on safeguarding crypto assets. As a result of these control failures, the FTX Group exposed crypto assets under its control to a grave risk of loss, misuse, and compromise, and lacked a reasonable ability to prevent, detect, respond to, or recover from a significant cybersecurity incident, including the November 2022 Breach.

1. Lack of Key Personnel, Departments, and Policies

While the FTX Group employed software developers and a single dedicated IT professional, it had no dedicated personnel in cybersecurity, a specialized discipline that generally acts as a "check" to mitigate risks posed by business pressure for technology to operate as fast and easily as possible. The FTX Group had no independent Chief Information Security Officer, no employee with appropriate training or experience tasked with fulfilling the responsibilities of such a role, and no established processes for assessing cyber risk, implementing security controls, or responding to cyber incidents in real time. Instead, its security was largely managed by Singh and Wang, neither of whom had the training or experience to handle the FTX Group's cybersecurity needs, and both of whom had responsibilities for the speed, efficiency, and continuing development of the FTX Group's technology, which are business needs that generally run counter to those of security and thus are

not appropriately managed by the same personnel. In short, as with critical controls in other areas, the FTX Group grossly deprioritized and ignored cybersecurity controls, a remarkable fact given that, in essence, the FTX Group's entire business—its assets, infrastructure, and intellectual property—consisted of computer code and technology.

2. Crypto Asset Management and Security

A critical responsibility of a crypto exchange, as with any business that holds funds provided by others, is to safeguard crypto assets from loss, misuse, misappropriation, or theft by insiders or unauthorized third parties. Crypto exchanges face unique security challenges in this regard, which only heightens their need to focus adequate time, resources, and expertise on fulfilling this core responsibility.

a. Crypto wallets and storage

Crypto assets are held in a crypto wallet, which consists of (i) a public key that serves as the asset owner's identifier on the blockchain ledger, and (ii) a private key that is required to access the user's crypto holdings, authorize transactions, and exercise ownership over a blockchain asset. A crypto wallet can either be a "cold" wallet (*i.e.*, an offline storage unit[22]) or a "hot" wallet (*i.e.*, a storage unit that is connected to the internet). Crypto assets held in hot wallets are at a higher risk of compromise because hot wallets are internet-connected, rendering their private keys vulnerable to hacking, malware, and other cybersecurity threats. Compounding the risk, blockchain transactions are generally irreversible and anonymous, making unauthorized transfers particularly challenging, if not impossible, to recover. For these reasons, it is axiomatic in the crypto industry that a private key should be kept confidential,

[22] Assets maintained in cold wallets are typically kept in a physically secured location and accessed only by authorized personnel on a need-to-access basis, a method known as "cold storage."

including by being generated and stored in a secure and encrypted manner,[23] and used exclusively by the owner. Relatedly, businesses that control private keys need detailed access control policies such that the keys may only be accessed by authorized parties or systems.

The FTX Group stored the private keys to its crypto assets in its cloud computing environment, which included over one thousand servers and related system architecture, services, and databases that it leased from Amazon Web Services (the "AWS account"). AWS's cloud computing platform offers businesses a range of infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) capabilities, and through it, like other businesses, the FTX Group customized, configured, and controlled its own cloud environment.

b. Lack of security controls to protect crypto assets

The FTX Group failed to implement basic, widely accepted security controls to protect crypto assets. Each failure was egregious in the context of a business entrusted with customer transactions, and any one of the controls may have prevented the loss in the November 2022 Breach. Taken together, the failures were further magnified, since each control failure exacerbated the risk posed by the others.

First, the FTX Group kept virtually all crypto assets in hot wallets, which are far more susceptible to hacking, theft, misappropriation, and inadvertent loss than cold wallets because hot wallets are internet-connected. Prudently-operated crypto exchanges keep the vast majority of crypto assets in cold wallets, which are not connected to the internet, and maintain in hot wallets only the limited amount necessary for daily operation, trading, and anticipated

[23] Encryption is the process by which readable data is converted to an unreadable form to prevent unauthorized parties from viewing or using it. Plaintext, by contrast, refers to data that is unencrypted and, therefore, can be viewed or used without requiring a key or other decryption device.

customer withdrawals.[24] Relatedly, prudently-operated crypto exchanges implement strict processes and controls to minimize the security risks (for example, the risk of hacking, theft or loss) inherent in the transfer of crypto assets between hot and cold wallets.

The FTX Group undoubtedly recognized how a prudent crypto exchange should operate, because when asked by third parties to describe the extent to which it used cold storage, it lied. For example, in 2019, Bankman-Fried falsely responded to a customer question on Twitter by providing assurance that "[we use the] standard hot wallet/cold wallet setup."[25] In 2022, the FTX Group responded to questions posed by certain advisers and counterparties about its use of cold storage as follows:

> FTX uses a best practice hot wallet and cold wallet standard solution for the custody of virtual assets. The firm aims to maintain sufficient virtual assets in the hot wallet to cover two days of trading activities, which means only a small proportion of assets held are exposed to the internet, the remaining assets are stored offline in air gapped encrypted laptops, which are geographically distributed. The 2-day trading figure is continuously monitored and if the hot wallet exceeds this amount, it will overflow into the cold wallet. If the figure drops below the 2-day trading figure, the hot wallet will be topped up from the cold wallet.

These representations were false. None of FTX.com, FTX.US, or Alameda had a system in place to monitor or move to cold wallets crypto assets in excess of the amount needed to cover two days of trading activity, and they did not use offline, air-gapped, encrypted, and geographically distributed laptops to secure crypto assets.

---

[24] Although there is currently no regulation in the United States that requires exchanges to use cold wallets to store customer assets, other regulatory authorities have imposed such requirements. For instance, regulation in Japan mandates that "Crypto Asset Exchange Service Providers" keep at least 95% of users' crypto assets in a device that is always disconnected from the internet. *See* Article 63-11(2) Payment Services Act in connection with Article 27(2) Cabinet Order on Crypto Asset Exchanges. Offline storage of information is also a standard security practice and control for organizations outlined in the U.S. National Institute of Standards and Technology ("NIST")'s Special Publication 800-53 under System and Communications Protection SC-28(2).

[25] Sam Bankman-Fried, (@SBF_FTX), Twitter (Aug. 16, 2019, 5:00 AM), https://twitter.com/SBF_FTX/status/1162288084634836993.

FTX Group employees openly acknowledged uncertainty about FTX Group's use of cold storage, and that regulators and users appeared to receive different information on the subject. In Slack communications in October 2022, an FTX Group employee relayed an internal communication that "it's ab[ou]t 70% cold and 30% hot," and that he had been instructed that this information was not to be shared with regulators unless it was specifically requested. Another FTX Group employee responded that if the question was being posed by "non-regulators," then "we say 10% in hot wallet, and 90% in cold wallet."

In fact, neither of these assertions about cold storage use was true. Outside of Japan, where required by regulation to use cold storage, the FTX Group made little use of cold storage. The Debtors have identified evidence that an individual associated with LedgerX, a non-Debtor entity, recommended to FTX Group management that FTX.US secure crypto assets in cold storage using a system similar to that employed by LedgerX, but no such system was put in place prior to the bankruptcy.

Second, the FTX Group failed to employ multi-signature capabilities or Multi-Party Computation ("MPC") controls (together, "multi-signature/MPC controls") that are widely used throughout the crypto industry to protect crypto assets. These controls require the cooperation of multiple individuals using unique keys or key fragments to effectuate a transaction.[26] As a result, the controls significantly reduce the risk of fraud, theft, misuse, or errors either by any single individual or in the event any single individual's key or key fragment is compromised. These controls are widely understood to be crucial for crypto exchanges to ensure that unauthorized transactions do not occur, for many reasons: exchanges are regularly

[26] "Multi-signature" refers to the requirement that two or more authorized individuals provide unique keys or credentials to perform sensitive or critical operations, such as engaging in a high-value transfer of crypto assets. MPC controls generate multiple private keys required to digitally sign transactions, thus providing multi-signature capabilities to crypto assets that do not natively support multi-signature. Because MPCs utilize cryptographic methods, multiple parties can act to effect a single transaction without revealing their private keys to each other.

targeted by hackers; exchanges custody assets provided by others, heightening the need for security; exchanges engage in a high volume of transactions, increasing the likelihood that errors will occur; and, as noted above, compounding all of these issues, crypto assets may be difficult or impossible to recover once they have been transferred.

While a single-key mechanism may not be inappropriate for wallets holding a relatively small amount of assets, such as those held by many retail customers, there is no question that a crypto exchange should employ multi-signature/MPC controls and cold storage solutions for—at a minimum—the central wallets that hold the majority of the crypto assets of the exchange. Nonetheless, neither the FTX exchanges nor Alameda utilized them to protect crypto assets. In the few instances in which the FTX Group even attempted to employ these controls, it misapplied them: for each wallet, the FTX Group stored together, in one place, all three private keys required to authorize a transfer such that any individual who had access to one had access to all the keys required to transfer the contents of the wallet, thus defeating the purpose of the controls.

Third, the FTX Group failed to manage or implement any appropriate system to attempt to manage private keys. As noted above, because crypto assets in a hot wallet may be misappropriated by anyone with access to the private key for that wallet, private keys must be maintained in a highly-secure manner. For crypto exchanges, controls to protect and manage keys are of paramount importance because customers who transfer crypto assets from their own wallets to the exchange's wallet must relinquish control over the security of their assets to the exchange. Exchanges and other crypto businesses rely on a variety of methods of secure key storage and management that are generally not difficult to implement, and they rely on detailed access control and management policies such that the keys may only be accessed by authorized

parties or systems critical to the operation of the associated wallets.[27] Businesses also regularly retain the services of third-party crypto custodians to secure their crypto assets and minimize the risk of maintaining their own private keys.

Despite the well-understood risks, private keys and seed phrases[28] used by FTX.com, FTX.US, and Alameda were stored in various locations throughout the FTX Group's computing environment in a disorganized fashion, using a variety of insecure methods and without any uniform or documented procedure. Among other examples:

- The Debtors identified private keys to over $100 million in Ethereum assets stored in plain text and without encryption on an FTX Group server.
- The Debtors identified private keys, as well as credentials to third-party exchanges, that enabled access to tens of millions of dollars in crypto assets that were stored in plain text and without encryption across multiple servers from which they could be accessed by many other servers and users in many locations.
- Single-signature-based private keys to billions of dollars in crypto assets were stored in AWS Secrets Manager (a cloud-based tool used to manage sensitive information), and/or a password vault (a tool for secure storage of passwords), neither of which is designed to meet the needs of secure-key storage; any of the many FTX Group employees who had access to AWS Secrets Manager or the password vault could access certain of the keys and unilaterally transfer the corresponding assets.[29]
- Alameda also lacked appropriate documentation as to the description or usage of private keys. For example, a key for $600 million dollars' worth of crypto assets was titled with four non-descriptive words, and stored with no information about what the key was for, or who might have relevant information about it. The Debtors identified other keys to millions of dollars in crypto assets that were simply titled "use this" or "do not use," with no further context.

---

[27] Examples of these methods include encryption, as well as the use of commercially available products such as hardware wallets, hardware security modules ("HSMs"), and MPC protocols. A hardware wallet stores a user's private keys in a secure hardware device that resembles a USB drive. Crypto transactions can be made by plugging the hardware wallet into a computer or other device. An HSM is a physical computing device that protects, manages, and stores secrets, such as cryptographic keys.

[28] A seed phrase (also known as a recovery phrase or mnemonic seed) is a series of words generated by a crypto wallet that allows a user to recover all the crypto assets associated with that wallet.

[29] In the infrequent instances in which the FTX Group stored private keys in encrypted form, it stored the decryption key in AWS Secrets Manager and not in a protected form, such as HSM. As a result, the decryption keys could easily be retrieved by an unauthorized actor, thereby dramatically reducing the value of encryption.

- Many FTX Group private keys were stored without appropriate backup procedures such that if the key was lost, the associated crypto assets would likely be permanently lost.

- Because the FTX Group lacked adequate records of private keys, there was a significant risk that crypto assets would be lost simply because no one knew how to locate or access them. As described below, through painstaking analysis by experts, the Debtors have recovered to date over a billion dollars' worth of crypto assets as to which few or no records existed.

- Because the FTX Group failed to maintain appropriate records of access to private keys, employees or others could potentially copy those keys to their own electronic devices and transfer the associated crypto assets without detection.

Fourth, the FTX Group failed to appropriately implement controls to manage "wallet nodes," which are software programs that operate on servers running the software of the blockchain network and help to implement and propagate transactions and maintain the security and integrity of the blockchain. A wallet node that holds private keys for a specific wallet is responsible for managing that wallet's assets and communicating with the blockchain network to process transactions. As a result, the security of the associated wallet's assets depends in large part on the security of the server on which the node is running.

Crypto exchanges typically use trusted wallet nodes to broadcast transactions and query the blockchain to reconcile exchange ledger data with blockchain data. The FTX exchanges and Alameda maintained servers that ran wallet nodes for blockchains, including Bitcoin, Litecoin, and Dogecoin, among others; these nodes acted as hot wallets that held hundreds of millions of dollars' worth of assets. Virtually all FTX.com Bitcoin assets, for example, were held in a single Bitcoin Core wallet node.

Despite the obvious importance of securing its wallet nodes, the FTX Group's security controls for its wallet nodes were grossly deficient. For example, the passwords for encrypting the private keys of wallet nodes were stored in plain text, committed to the code repository (where they could be viewed by many and were vulnerable to compromise), and

reused across different wallet nodes such that if one were compromised, every other node with the same password could be compromised as well. Furthermore, wallet node servers were not securely segregated from connected servers such that anyone who compromised the FTX Group's computing environment could potentially compromise its wallet nodes.

3. Identity and Access Management

The FTX Group failed to implement in an appropriate fashion even the most widely accepted controls relating to Identity and Access Management ("IAM")—often the first line of defense in preventing an unauthorized system compromise. IAM refers to the policies, technologies, and procedures used to manage digital identities and control access to computer systems. Typically, IAM controls involve user authentication, authorization, and permissions management to ensure that only authorized individuals or systems are granted access to resources, while preventing unauthorized access and enforcing security policies. In the context of a cryptocurrency exchange, IAM controls are essential for protecting the confidentiality, integrity, and availability of crypto assets.

The FTX Group's IAM controls were insufficient in at least three respects:

First, the FTX Group failed to adhere to the basic security principle of "least privilege," by which users and systems are given access to the minimum needed to perform their duties or functions and nothing more.[30] By limiting access in this way, the impact of a security breach or an unintentional action involving any particular user or system is also necessarily limited. Among notable examples of the FTX Group's failures in this respect, over a dozen people had direct or indirect access to the FTX.com and FTX.US central omnibus wallets, which

[30] The Committee on National Security Systems defines "least privilege" as "[t]he principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function." Committee on National Security Systems (CNSS) Glossary, CNSSI No. 4009-2015, (Apr. 6, 2015).

held billions of dollars in crypto assets, and dozens of other users were granted access to other types of FTX exchange and Alameda wallets. Only a small number of these individuals needed access to these wallets to perform their duties.

Second, the FTX Group failed to effectively enforce the use of multi-factor authentication ("MFA") among its own personnel and corporate infrastructure, increasing the risk that key account credentials would be compromised and critical assets would thereby be vulnerable to unauthorized access. MFA is a basic security mechanism that requires users to provide two or more methods of authentication (for example, a password and one-time passcode sent to a cell phone or email previously associated with the user) to verify their identity and gain access to a system or account. MFA is a widely used and simple technique to mitigate the risks created by password weaknesses and theft, and businesses commonly require MFA to access any corporate systems, and particularly systems holding sensitive data.

The FTX Group did not enforce the use of MFA in connection with two of its most critical corporate services—Google Workspace, its primary tool for email and document storage and collaboration, and 1Password, its password-management program. The deficiency is ironic given that the FTX Group recommended that customers use MFA on their own accounts,[31] and Bankman-Fried, via Twitter, publicly stressed the importance of "2FA [Two-factor authentication]," a form of MFA, for crypto security:

[31] *See* FTX.US Security Features, (Sept. 25, 2021) [http://web.archive.org/web/20210925211745/https:/help.ftx.us/hc/en-us/articles/4408447825815-FTX-US-Security-Features]; FTX.US Security Features, (Aug. 14, 2022) [http://web.archive.org/web/20220814000906/https:/help.ftx.us/hc/en-us/articles/4408447825815-FTX-US-Security-Features]; FTX Security Features, (Sept. 21, 2021) [http://web.archive.org/web/20210921181611/https:/help.ftx.com/hc/en-us/articles/360044838051-FTX-Security-Features-]; FTX Security Features, (July 1, 2022) [http://web.archive.org/web/20220701085013/https:/help.ftx.com/hc/en-us/articles/360044838051-FTX-Security-Features-].

> Daily reminder: use 2FA! 90% of crypto security is making sure you've done the basics.[32]

While he correctly characterized MFA as one of "the basics" in securing crypto assets, the FTX Group did not enforce it in the essential areas described above. And in an important instance in which FTX Group did use MFA—for a corporate email account that handled significant administrative matters—FTX Group management arranged to bypass the MFA requirement.

Third, the FTX Group generally did not use Single Sign-On ("SSO"),[33] an authentication scheme used by companies worldwide to manage user access centrally, enabling users to adopt a single strong password to use across multiple applications, thus reducing the risk of unauthorized access and other harms. Without SSO, among other problems, the FTX Group could not effectively manage or revoke user access, enforce MFA, revoke user access, or prevent users from having many user accounts for different services with separate passwords, which increased the likelihood of compromise.

4. Cloud and Infrastructure Security

The FTX Group also failed to implement appropriate controls with respect to cloud and infrastructure security—that is, controls to protect its cloud services, networks, servers, and "user endpoints" such as desktops and laptops. These controls were crucial for the FTX Group, which essentially "lived" in the cloud, where the exchanges operated and the FTX

---

[32] Sam Bankman-Fried, (@SBF_FTX), TWITTER (Sept. 12, 2019, 4:11 AM), https://twitter.com/SBF_FTX/status/1172060173604515840.

[33] SSO enables users to authenticate their identity once in order to continually gain access to multiple applications and services without having to re-enter login credentials.

Group stored the majority of its assets. The FTX Group's management of its cloud and infrastructure security deviated from standard corporate practices in several respects.

First, the FTX Group generally shared computer infrastructure and IT services among FTX.com, FTX.US, and Alameda, and in doing so, departed from the fundamental security principle of segmentation, whereby business entities and computing environments are separated to minimize the impact of a breach, and exercise greater control over who can access particular systems. Among many examples, the FTX exchanges and Alameda used a single, shared AWS account, meaning that a compromise of that AWS account would expose all three entities' assets to misuse or theft.[34]

Second, while crypto exchanges are notoriously targeted by hackers, the FTX Group had poor or, in some cases, no "visibility" controls to detect and respond to cybersecurity threats. As widely understood across industries, and emphasized by the U.S. government in public advisories, appropriate visibility controls generally include the creation and collection of logs that record and reflect activity within the computing environment, and systems to alert

[34] Other significant examples of the FTX Group's segmentation failures that increased the risk of harm from an information security problem or compromise include hosting FTX.com and Alameda in the same collaboration platform, Google Workspace, and employing the same password vault tenant, 1Password, for both FTX.com and FTX.US. The FTX Group appears to have recognized the deficiency, because as of the petition date, FTX.US had begun a process of migrating to its own dedicated AWS account; because it did not complete that work, its assets remained within the shared account such that FTX.US lost approximately $139 million of its crypto assets during the November 2022 Breach. In these ways, the FTX Group departed from best practices, which call for segregation and separation of an organization's infrastructure and networks in order to effectively mitigate the risk of, and impact from, unauthorized access to the organization's environment. *See, e.g.*, U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Securing Network Infrastructure Devices*, at https://www.cisa.gov/news-events/news/securing-network-infrastructure-devices (noting that "[s]ecurity architects must consider the overall infrastructure layout, including segmentation and segregation" because "[a] securely segregated network can contain malicious occurrences, reducing the impact from intruders in the event that they have gained a foothold somewhere inside the network").

designated personnel to suspicious activity.[35] The FTX Group failed by any measure to maintain such appropriate controls.

Among many examples of its control deficiencies in this area, the FTX Group did not have any mechanism to identify promptly if someone accessed the private keys of central exchange wallets holding hundreds of millions or billions of dollars in crypto assets, and it did not fully enable even the basic features offered by AWS to assist with cyber threat detection and response.[36] In fact, due to the lack of such controls, the FTX Group did not learn of the November 2022 Breach until the Debtors' restructuring advisor alerted employees after observing, via Twitter and other public sources, that suspicious transfers appeared to have occurred from FTX Group crypto wallets. The FTX Group similarly failed to institute any basic mechanism to be alerted to any "root" login to its AWS account, the cloud computing environment where it operated the FTX exchanges and stored keys to billions of dollars in crypto assets, even though such access would provide virtually complete access to the environment.

Third, the FTX Group did not implement controls sufficient to protect its network endpoints, such as laptops and desktops, from potential security threats. The FTX Group had no commonly used technical controls to ensure that employees used their corporate laptops, leaving employees free to use personal devices devoid of corporate security controls. The FTX Group also lacked any endpoint protection tool to monitor cloud-hosted servers for threats, and several

---

[35] *See, e.g.*, U.S. CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY, *Weak Security Controls and Practices Routinely Exploited for Initial Access* (last revised Dec. 8, 2022), at https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-137a (noting that "[l]og files play a key role in detecting attacks and dealing with incidents[,]" that "implementing robust log collection and retention" provides organizations with "sufficient information to investigate incidents and detect threat actor behavior," and that effective log management calls for setting up "notifications of suspicious login attempts based on an analysis of log files").

[36] For example, Amazon GuardDuty, an AWS feature that supports threat detection, was not enabled at all on FTX.com, and across the entities, VPC flow logs that can capture IP traffic information were only enabled to log the rejected traffic (and only in some networks)—they were not enabled to log the permitted traffic at all. The lack of these and other logs complicated the Debtors' investigation of the November 2022 Breach.

of its critical services did not have the latest security updates installed. For example, to manage inbound internet traffic on a key server, the FTX Group used a version of software that was nearly four years out of date, leaving the server exposed to known vulnerabilities that had been addressed in updated versions of the software. This practice flouted industry standards by which software flaws and vulnerabilities should be remediated in a timely manner.[37]

Fourth, the FTX Group had no comprehensive record from which it could even identify critical assets and services, including employee workstations, software application servers, business data, and third-party cloud and other services it relied upon, leaving it with little to no visibility into what it needed to secure, let alone how to best secure it.[38] Indeed, to understand and gain necessary access to the full scope of services that the FTX Group used, the Debtors had to analyze financial records such as bills paid to vendors, and search through employees' email and chat messages. Although the FTX Group's designated IT professional began creating an inventory of electronic devices issued to employees, and stressed to Singh (who was supposedly in charge of the FTX's Group's cybersecurity) the importance for security purposes of having Singh and other FTX Group senior management identify in the inventory the electronic devices they were using, neither Singh nor other senior management provided the requested information.

5. Application and Code Security

The FTX Group did not implement controls sufficient to protect sensitive data relating to its applications, including its application code, from vulnerabilities and attacks. While essential in any context, securing such data was particularly critical for the FTX Group, which

---

37 *See* NIST Special Publication 800-53 Revision 5: SI-2: Flaw Remediation.

38 The NIST identifies the development and maintenance of an inventory of information systems (including hardware, software, and firmware) that are owned, leased, or operated by an organization as a standard security practice and control. *See* NIST Special Publication 800-53 Revision 5: PM-5: Information System Inventory.

used multiple applications with access to sensitive data and assets, including customer data, financial data, and crypto wallets. In managing its application and code security, the FTX Group departed from standard practices in several ways.

First, while it is widely recognized that sensitive data should be protected through encryption and appropriate access controls,[39] the FTX Group failed to adopt these basic controls to secure its "application secrets," that is, the highly sensitive data such as passwords, API keys,[40] and private keys used by its applications. Protecting these secrets is paramount because they are frequently the target of malicious actors who may use them to gain access to additional data and assets. With respect to the FTX Group, access to such secrets could enable someone to make transfers of billions of dollars' worth of crypto assets from hot wallets or third-party crypto exchanges. Nonetheless, among many examples of its deficient controls in this area, the FTX Group simply stored certain secrets—including the private keys and seeds to Alameda's crypto wallets—in unencrypted files to which numerous employees had access, and kept hundreds of other secrets—including passwords for crypto wallet nodes, API keys for crypto exchanges, and credentials for sensitive email accounts—in source code repositories from which they were widely accessible.[41]

---

[39] *See* NIST Special Publication 800-53 Revision 5: SC-28: Protection of Information at Rest.

[40] Application Programming Interface, or "API," keys are credentials used to authenticate to third-party services, including, for example, other crypto exchanges.

[41] While a senior developer subsequently deleted a file containing these secrets from the repository, the developer did not remove the file from the code history in the repository, contrary to the recommended practice of GitHub, where the repository was maintained. As a result, the file continued to remain exposed to anyone who accessed the code repository.

Second, the FTX Group failed to adopt certain standard controls in order to ensure the integrity of its code.[42] For example, there was no effective process for securely introducing, updating, or patching software, and no procedures, such as scanning, to continually ensure the integrity of the code running on FTX Group servers. Thus, among many other harms, the FTX Group was highly vulnerable to software "supply chain" attacks in which malicious actors insert vulnerabilities into third-party software in order to compromise any organization that uses the software.[43] Furthermore, with only minimal code review and testing procedures in place, and no focus on continuous security testing, the FTX Group did not review, test, or otherwise deploy its code in a manner that sufficiently ensured that it was functioning as expected and free of vulnerabilities that might be leveraged by malicious actors.

6. Debtors' Work to Identify and Secure Crypto Assets in the Computing Environment

As a result of FTX Group's lack of appropriate documentation and recordkeeping, the Debtors had to undertake significant efforts to identify, access, and secure crypto assets from the FTX Group's computing environment. The lack of records was particularly challenging because cryptocurrency keys are simply strings of alphanumeric characters that may otherwise be indiscernible in a computing environment. The Debtors' challenge was compounded by the

---

[42] *See, e.g.,* NIST Special Publication 800-53 Revision 5: SA-12: Supply Chain Protection ("Verify the integrity of code obtained from external sources before it is deployed on the system"); NIST Special Publication 800-53 Revision 5: SA-11: Developer Security Testing and Evaluation ("Require developers to test their code for security vulnerabilities before it is deployed into production"); NIST Special Publication 800-53 Revision 5: SA-3: System Development Life Cycle ("Incorporate security requirements into the system development life cycle and ensure that security is addressed in all stages of the life cycle").

[43] The most prominent example of a software supply chain attack is the 2020 SolarWinds attack, in which Russian state-sponsored actors compromised SolarWinds software, used widely throughout the U.S. public and private sectors, in order to gain access to the networks of government agencies and companies that downloaded the software.

enormous time pressure that they faced due to a confluence of circumstances that resulted from other FTX Group control failures described above:

- The Debtors took over responsibility for a computing environment that had been compromised. A malicious actor had just drained approximately $432 million worth of crypto assets in hours; the FTX Group did not have the controls to detect the compromise, much less to stop it; and due to the FTX Group's deficient controls to secure crypto assets, the Debtors faced the threat that billions of dollars of additional assets could be lost at any moment.

- Compounding the challenge, and reflecting additional FTX Group control deficiencies, the Debtors' cybersecurity experts found that the FTX Group had no written plans, processes, or procedures that explained the architecture or operation of its computing environment or storage of crypto assets.

- Even as they raced to secure the environment in these challenging circumstances, the Debtors separately faced the risk that individuals in possession of private keys to crypto assets could unilaterally transfer those assets. In other words, securing the environment would not be enough: until the crypto assets were transferred to cold storage, they could be taken by anyone who had the private keys. Indeed, the day after the November 2022 Breach, without the Debtors' authorization, and at the direction of Bahamian authorities, Bankman-Fried and/or Wang used private keys they had in their possession to transfer hundreds of millions of dollars' worth of FTT, SRM, MAPS and other tokens out of Debtor wallets and into cold wallets in Bahamian custody.[44]

- Compounding all of these challenges, and as the Debtors worked to identify and access crypto assets with no "map" to guide them, the Debtors had to engineer technological pathways to transfer many types of assets they identified to cold storage because the FTX Group had never engaged in the computer engineering necessary to make those transfers possible.

The Debtors' work to identify and secure these crypto assets required the combined efforts of experts in computer engineering, cryptography, blockchain technology, cybersecurity, IT architecture, and cloud computing. Examples of the work that was undertaken to identify crypto assets in the environment—ultimately, to date, over a billion dollars' worth of crypto assets as to which few or no records existed—include the following:

[44] Due to price declines, illiquidity, and other issues, these tokens are currently worth a small fraction of the amount of their estimated worth at the time of transfer.

- Experts developed novel code to identify crypto assets and keys that were stored in over a thousand servers and IT resources that constituted the FTX Group computing environment. Millions of these keys had no labelling or description that reflected their nature or use, requiring further analysis and blockchain analytics. Through this work, the Debtors recovered hundreds of millions of dollars' worth of crypto assets not reflected in any recordkeeping system of the FTX Group.

- Experts identified and recovered crypto wallets used for the FTX Group's extensive trading operations, and developed scanning tools and dedicated software to identify Alameda's DeFi portfolio[45] as to which few centralized records have been identified. Using these tools, the Debtors have identified tens of millions of dollars' worth of crypto assets that are in the process of being recovered.

- Experts learned that the FTX exchanges had experienced difficulty with the accuracy of code that the FTX Group had engineered to identify and transfer assets from over 10 million wallets of exchange customers into omnibus accounts. Surmising that crypto assets could still remain scattered among the wallets due to the inaccuracy of that code, experts developed code that would automatically both identify any crypto assets across blockchains that remained among the more than 10 million wallets, and then automatically transfer those assets to cold storage. Through the operation of this code alone, the Debtors have identified and secured over $140 million in crypto assets of the estate.

V. Conclusion

The FTX Group's profound control failures placed its crypto assets and funds at risk from the outset. They also complicated the Debtors' recovery efforts, although the Debtors have made and continue to make substantial progress in that regard. To date, through the work described above, the Debtors have recovered and secured in cold storage over $1.4 billion in digital assets, and have identified an additional $1.7 billion in digital assets that they are in the process of recovering. The Debtors will continue to provide updates on their ongoing recovery efforts and investigation.

[45] A Decentralized Finance (DeFi) portfolio encompasses a range of investments, holdings, and trading positions in blockchain-based financial applications that operate in a decentralized, peer-to-peer manner, rather than relying on centralized exchanges, brokerage firms, or banks.